

⑫ 公開特許公報 (A) 昭62-189

⑤ Int.CI.

H 04 N
7/16
7/10
7/20

識別記号

府内整理番号

7013-5C
7013-5C
7013-5C

⑪ 公開 昭和62年(1987)1月6日

審査請求 未請求 発明の数 1 (全7頁)

⑩ 発明の名称 有料放送方式

⑪ 特願 昭60-137961

⑫ 出願 昭60(1985)6月26日

⑬ 発明者 坂本 義明 深谷市幡羅町1-9-2 株式会社東芝深谷工場内

⑭ 出願人 株式会社東芝 川崎市幸区堀川町72番地

⑮ 代理人 弁理士 则近 憲佑 外1名

明細書

1. 発明の名称

有料放送方式

2. 特許請求の範囲

放送局側において、有料放送番組に対応した番組種別情報を発生する番組種別情報発生手段と、前記有料番組放送を加入者が契約したことを示す契約番組種別情報発生手段と、

前記有料放送信号に対してスクランブルを行なうための鍵情報を生成する鍵情報生成手段と、

前記鍵情報を生成する鍵情報生成手段と、前記番組種別情報を送出する送出手段とを有し、

受信側において、前記番組種別情報、及び前記契約番組種別情報を抽出する抽出手段と、

前記鍵情報を抽出する鍵情報抽出手段と、

前記契約番組種別情報と番組種別情報との比較を行なう比較手段と、

この比較手段によって前記契約番組種別情報と番組種別情報との対応が検出されない場合、信号音を出力して加入者が当該有料番組に対し未契約

であることを音声で知らせる未契約警告手段とを有したことを特徴とする有料放送方式。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、例えば放送衛星等を用いた空中線又は伝送線を介するCATVに代替される有線形態で映像、音声、データ、图形情報をサービスする形態において視聴を契約した加入者のみにサービスを行なう有料放送方式に係り、特に加入者が番組予約をし忘れた場合等で受信できないとき機器の故障ではなく予約していないことに基づいてディスクランブルのための鍵情報が生成されていないことを知らせる有料放送方式に関するもの。

〔発明の技術的背景とその問題点〕

近年、新放送メディアの発達とともに、テレキスト、静止画放送、高品位テレビジョン放送、デジタル倍速による多チャンネル放送が可能となってきている。このような放送メディアの高度化により放送番組の伝送種類も多岐にわたってきている。

そして、放送局側においては特定番組に対して課金を行ない放送局側と契約を行なった特定の加入者以外の加入者に対しては伝送信号に対して攪拌を与える。いわゆるスクランブルを行ない視聴を阻止し、契約加入者に対してはこのスクランブルを解除することによって視聴を可能にする有料放送が有料番組に対して行なわれる。

この場合、有料放送方式において加入者が有料番組を予約するには識別符号(ID)とともに所望の番組を予約する訳であるが、実際の加入者以外の名義で不正予約を防ぐ意味において当該契約者固有の識別信号(ID)を放送局側に告知することを番組予約時に行なわせるシステムが採用される。即ち、識別信号(ID)及び予約対象番組を示す公開鍵であるティア(T1)と呼ばれる情報で放送局側に番組予約をし、放送局側ではこれらの公開情報を秘匿情報に変換してどの加入者が契約したかの情報及び信号に対するスクランブルを解くための情報の両者を秘匿する。この秘匿情報は加入者側に送られ、この秘匿情報より復号化鍵を生成し暗号

よって加入者に上記鍵が与えられていないことを知らせる必要がある。

即ち、予約を完了していない番組を加入者が選定したときには未予約であることを加入者に認知させることが望まれる。

〔発明の目的〕

この発明は上記の点に鑑みなされたものであり加入者の予約作業によってスクランブルを解くための鍵が当該加入者に与えられないときには、未契約である旨を加入者に認知させることのできる有料放送方式を提供することを目的とする。

〔発明の概要〕

この発明に係る有料放送方式では、例えば第1図に示すように放送局側100では、データメモリ60に有料番組の種別を示す予約ティア情報(T1)及び有料番組に対してスクランブルするための鍵情報が格納されており、この鍵情報を用いて乱数発生器10で乱数を発生させ有料放送信号を排他的論理和回路210でスクランブルする。また、データメモリ70には加入者識別符号(ID)に対応し

化された情報を平文化して復号を行なう。

このような有料方式においては上記したように放送局側に対する番組予約は公開鍵を用いて行なう放送局側で課金に対する検査を行なった後に暗号化された情報を平文化するに必要な情報が加入者側にダウンロードされる。

上記有料放送方式においては、予約番組情報であるティア(T1)を放送局側に登録することで予約がなされ、有料放送の視聴を可能にする鍵情報が当該加入者に対して設定されて当該有料放送に対する加入者の視聴を可能にする。このため予約動作によってスクランブルを解くため鍵情報が設定されないと、加入者は当該有料番組の視聴ができない。この場合、加入者の予約(契約)し忘れによる原因か或は機器の故障原因のいずれの原因により加入者が視聴できないのか加入者には判別できない。

そこでスクランブルを解く為の鍵が加入者側で得られない場合には加入者にこれを知らせ、故障によって視聴できないのではなく予約のし忘れに

て当該加入者が契約している場合には該当契約有料番組の種別を示す予約ティア(T1)として格納される。

加入者側200では予約ティア(T1)は鍵抽出回路223で抽出され、受信ティア(T1)は鍵抽出回路228で抽出され、両ティア(T1)は比較器229で比較される。比較の結果、両ティア(T1)が一致しない場合にはCPU300は、スイッチ900にて回路を信号発生回路800に切替えて信号音出力させる。この信号音によって加入者側に対して未契約であることを知らせる。

また、この場合、制御回路230は復号器231の復合動作を停止させ乱数発生器220での復号のための乱数の発生が停止される。

〔発明の実施例〕

以下、この発明の一実施例を図面を参照して説明する。

第2図はこの発明に係る有料放送方式の一実施例を示す回路図である。この第2図に示す回路によって放送信号に対するスクランブルによって伝

送信号に対する暗号化がなされるが、課金対象となるデジタル放送情報は入力端子 IN に印加される。

この放送情報は有料放送としてスクランブル処理され加入者に対してのみ復号がなされるよう乱数発生器 10 で発生した乱数を用いて排他的論理和回路 20 でスクランブル処理がなされる。この排他的論理和回路 20 の出力に得られるスクランブル化された放送情報は、契約加入者に対してのみ復号が許可されるが、復号のために必要な情報を放送局側 100 から加入者側 200 に伝送する必要がある。

上記したように、放送信号自体は上記模似ランダム雜音を発生する乱数発生器 10 の動作により秘匿されるが、どの契約者にどのような番組の視聴を許可するかの復号可能契約者を特定する情報も秘匿する必要がある。このように、番組情報自体を秘匿するための秘匿鍵情報、復号可能契約者を特定するための秘匿鍵情報の 2 種の暗号鍵としての秘匿鍵情報により有料化がなされる。

（KI）は、メモリテーブル 60 に形成されたチャンネル番号毎に付され番組ジャンルを示すティア（Ti）及びこのティア（Ti）Kc 対して付された暗号ティアキー（Ki）からなるメモリマップより抽出され上記乱数発生器 10 に与えられる。この結果、上記乱数発生器 10 は、上述の 2 種類の暗号鍵であるイニシャルデータ（In）、ティアキー（Ki）を用いて $K_s = f(K_i, In)$ なる乱数を発生する。この乱数 K_s は一方入力端に放送情報が加えられる排他的論理和回路 20 の他方入力端に加えられ、スクランブル化された放送情報が得られる。この場合、上記イニシャルデータ（In）は、スクランブル化された放送情報を平文化するため、暗号鍵情報として用いられるので、イニシャルデータ自体も加入者側にダウンロードされる。

放送局側では、どの加入者がどの番組に対して契約しているかの情報を暗号文として生成するがこの情報もダウンロードして加入者側での復号のための鍵情報（EI）として用いられる。この暗号情報（EI）はメモリテーブル 70 に形成された各加入

このような有料放送システムにおいては、加入者を示す識別符号（ID）、及び予約番組の種類を示すティア（Ti）の公開鍵情報、上記乱数発生器 10 に対する初期値（In）、上記ティア（Ti）に対する暗号符号であるティアキー（Ki）、上記識別符号（ID）に対応するパスワード（Pa）が非公開の暗号鍵として扱われる。

先ず、放送情報を秘匿化する乱数発生器 10 について述べると、この乱数発生器は例えば M 系列符号発生器等で構成され所定のアルゴリズムによる乱数が発生する。この場合乱数発生器 10 の初期値は同期信号発生回路 30 で発生するタイミング信号にもとづき、制御回路 40 の制御のもとにイニシャルデータ発生回路 50 によって発生する。このイニシャルデータ（In）は上記ティアキー（Ki）とあいまって上記乱数発生器 10 のシーケンス動作を制御する。

即ち、上記乱数発生器 10 とシーケンス動作は上記イニシャルデータ（In）とティアキー（Ki）によって制御を受けるわけであるが、上記ティアキ

ーを識別する識別符号（ID）に対応して付された秘匿情報であるパスワード（Pa）と上記ティアキー（Ki）とにより $EI = g(K_i, Pa)$ として暗号器 80 で生成される。暗号情報（EI）も加入者側でスクランブル化された放送情報を復文化するため鍵情報として用いられるので、この暗号情報（EI）を復号できない加入者はスクランブル化された放送情報をディスクランブルして放送信号を受信することはできない。従って、課金マップ 90 を CPU 110 が参照し、CPU 110 は料金未納等の契約対象外の者に対しては上記暗号情報（EI）を作成せず当該加入者は放送の視聴が禁止される。

このように放送局側 100 からは、第 1 の鍵情報 K_s でスクランブル化された放送情報、契約加入者を特定するに供する第 2 の鍵情報 EI、及び上記乱数発生器 10 に対する初期値情報（In）がタイミング回路 120 によるタイミング制御のもとにモ뎀 130 を介して秘匿情報として加入者側 120 にダウンロードされる。更に、公開鍵である番組類似表示ティア（Ti）がダウンロードされる。

次に、加入者側 200についてみると、スクランブルされた放送情報は排他的論理和回路 210 の一方の入力端に加えられる。このスクランブルを解くには、上記乱数発生器 10 で発生した乱数と同じ乱数を上記排他的論理和回路 210 の他方の入力端に加えればよいが、この復号化は上述した第 1 の鍵情報 K_0 、第 2 の鍵情報 E_1 を生成して乱数発生器 220 でスクランブル時における乱数と同様の乱数を発生することで行なわれる。このようなディスクランブルに供する乱数を発生するには上記第 1 の鍵情報を生成する必要があるが、加入者側では第 1 の鍵情報 K_0 を再生するためにはティアキー (K_1)、イニシャルデータ (In) を抽出することが必要になる。この場合、ティアキー (K_1) は、ダウンロード時に第 2 の鍵情報 E_1 で暗号化されているため、ティアキー (K_1) を直接抽出できず一旦第 2 の鍵情報 (E_1) を抽出しこれからティアキー (K_1) を抽出する処理が行なわれなければならない。

ディスクランブル動作を説明するに、先ず、データ処理に必要な同期信号は同期信号抜取り回路

との比較を比較器 229 で行ない。この比較の結果ティアが一致している場合には制御回路 230 によって復号器 231 を動作させる。このとき復号器 231 は上記 RAM 225 から読み出した鍵情報 (E_1) と上記 ROM 226 から読み出した加入者に付されたパスワード (P_a) から上記暗号器 80 と逆のデータ処理を行ないティアキー (K_1) を生成する。このティアキー (K_1) 及び上記鍵情報抽出回路 228 で抽出したイニシャルデータ (In) をもとに乱数発生器 220 でスクランブルに供する乱数と同様の乱数が発生する。この乱数は排他的論理和回路 210 に加えられ、ディスクランブル処理がなされ平文化された放送情報を出力端子 OUT に得る。

これらの一連のディスクランブルに関連するデータ処理は CPU 300 による制御による。

次に、契約加入者側 200 から加入者が放送局側 100 に対して契約を申し込む場合について述べる。

加入者が契約するには、先ず表示器 400 に表示された加入者識別符号 (ID) をキーパッド 500 を押して入力する。その後、加入者ははじめ知らさ

221 によって抽出され、この同期信号をもとにデータ処理に必要なタイミング信号をタイミング信号発生回路 222 が発生する。また、放送局側 100 から送られた関連鍵情報は鍵情報抽出回路 223 で抽出される。即ち、イニシャルデータ (In)、鍵情報 $E_1 = g(K_1, P_a)$ 、及びティア (T_1) が鍵情報抽出回路 223 で上記タイミング発生回路 222 で規定されるタイミングに従い抽出される。この抽出された関連鍵情報は RAM 書込制御回路 224 の制御信号の制御によって RAM 225 に書き込まれる。このとき、各加入者毎に付されている加入者識別符号 (ID) 及びパスワード (P_a) が加入者側の ROM 226 から読み出されたものと一致しているか否かを比較器 227 で判別し、比較の結果一致しているときのみ上記 RAM 225 に対し関連鍵情報の書き込みが許可される。

また、イニシャルデータ (ID)、公開鍵情報である番組想様を示すティア (T_1) は鍵情報抽出回路 228 で抽出され上記 RAM 225 に書き込まれたティア (T_1) と伝送された番組に付随するティア (T_1)

れている番組想様を示すティア (T_1) を上記キーパッド 500 を操作して入力し、番組予約を行なう。これらの加入者識別符号 (ID)、ティア (T_1) は CPU 300 で処理された後にモデム 600 を介してアップストリームによって放送局側 100 へ送られる。放送局側 100 では上記加入者からの予約情報である加入者識別符号 (ID)、ティア (T_1) はモデム 130 で復調された後、課金マップ 90 に加入者識別符号 (ID) をもとに課金情報を書き込む。そして CPU 110 は上記課金マップ 90 を参照し、料金支払い等を確認した後にメモリテーブル 60 に対して非公開情報であるティアキー (K_1) を書き込む。これにより予約処理が行なわれ、放送局側 100 から有料放送情報を入力端子 IN から送出する場合には排他的論理和回路 20 によってスクランブル処理が行なわれた信号が伝送され、加入者側 200 では契約加入者のみ排他的論理和回路 210 によってディスクランブルされる。

このように加入者が契約するにあたっては加入者は希望する番組想様に対応した情報であるティ

ア(TI)を放送局側100に送るわけであるが、加入者が上記ティア(TI)を放送局側100に予約情報として伝送しないと放送局側100ではデータメモリ60にスクランブルを解くための鍵情報の一つであるティアキー(KI)を書き込まない。このためディスクランブルに関係する鍵情報(EI)が暗号器80で形成されず、また加入者側200でディスクランブルに関連するティアキー(KI)は生成されない。これは、伝送されたティアキー(TI)と加入者が設定する予約ティア(TI)との一致が比較器229で検出されないことによる。

即ち、加入者が予約をしていないと、上記復号器231はディスクランブルのためのティアキー(TI)を生成できない。このときディスクランブル動作がなされないことで放送波の視聴ができない加入者は、機器の故障か予約のし忘れによって視聴できないのかの判別できない。また、音楽専用のレシーバー等は予約されていないとミュートがかかるものがあり、うつかり、アンプ等の音量を最大にしたまままで音が出た時にスピーカ等の機器

上記第3図に示した加入者側200では、伝送された鍵情報は鍵情報抽出回路223,228で抽出される。この鍵情報抽出回路228で抽出される鍵情報としてはイニシャルデータ(ID)、ティアキー(KI)と加入者識別符号(ID)に対応して付したパスワード(Pa)から生成した非公開鍵である(EI)及びティア(TI)がある。この場合ティア(TI)は放送局側100から送られるが、加入者が予約を行ない契約した番組であることを示す予約ティア(TI)と加入者の契約の有無に拘らず伝送される受信ティア(TI)の2種がある。この2種のうち、予約ティア(TI)は、加入者が契約したことで放送局側100でメモリテーブル60に契約によってティアキー(KI)が与えられたティア(TI)を示す。この予約ティア(TI)は加入者においては鍵情報抽出回路228によって上記タイミング信号発生回路222で発生するタイミング信号に従がい抽出される。

一方、加入者の契約の有無に拘らず、伝送番組とともに伝送番組の種類を示す信号として機能する受信ティア(TI)は鍵情報抽出回路228で抽出さ

れることがある。

そこで、この実施例では上記比較器229で比較結果をもとにCPU300を制御して、伝送されたティア(TI)と予約ティア(TI)とが一致しない場合には、スイッチ900を⑧側へ切替え、信号音発生回路800から、ティア(TI)が一致していないことを示す信号音（例えば正弦波等の間欠音）を出力する。これにより、機器の故障によるものではなく予約のし忘れ等によって復号器231が動作していないことによることを加入者に知らせる。

第3図は、第2図に示した実施例において、予約ティア(TI)と受信ティア(TI)との一致を検出し契約番組か否かの判別を行う回路の実施例を示す。なお、第2図と同一部分には同一符号を付しその説明を省略する。

第3図において伝送信号中に含まれる同期信号は同期信号抜取り回路221によって抽出され、この抽出された同期信号にもとづいて処理に必要なタイミング信号はタイミング信号発生回路222で発生する。

れる。この受信ティア(TI)は放送情報種別を示す情報として上記予約ティア(TI)とは異なる情報フレームに挿入して伝送される。

そして、上記鍵抽出回路223で抽出された予約ティア(TI)はRAM書き込み制御回路224を介してRAM225に書き込まれる。RAM225に書き込まれた予約ティア(TI)情報は比較器229の予約ティアレジスタ710に読み出される。また、上記受信ティア(TI)情報は受信ティアレジスタ720に置き換えられ、上記受信ティア、予約ティアの両者が一致しているか否かは比較器229の比較手段730によって検出される。即ち、伝送された番組情報が加入者が契約した番組であるか否かの判別が比較器229によってなされる。この場合、予約ティア(TI)と受信ティア(TI)が一致していないと、復号器231を制御する制御回路230の制御動作を停止させるとともにCPU300にティア(TI)の不一致を示す信号を供給する。この信号を受けたCPU300は、スイッチ900を⑧に切替え信号音発生回路800をティアの不一致を示すべく駆動する。

このディアの不一致を示す信号によって、加入者が当該放送情報を視聴できないのは未契約によるものであることが知らされる。

〔発明の効果〕

この発明に係る有料放送方式によれば、上述したように伝送番組に対して加入者が契約しているか否かをスクリンブル鍵情報を用いた制御によって加入者に認知させることができる。これにより、加入者は、当該放送が視聴できないのは未契約によることが認識できるし、音声信号を出すことでアンプ等の音量を上げっぱなしによるスピーカ等の破損をなくすことができる。

また、スクリンブルを解除するに関与する復号器を上記した未契約番組であるか否かを確認した上で制御するのでスクリンブル動作も確実な有料放送方式を提供し得るものである。

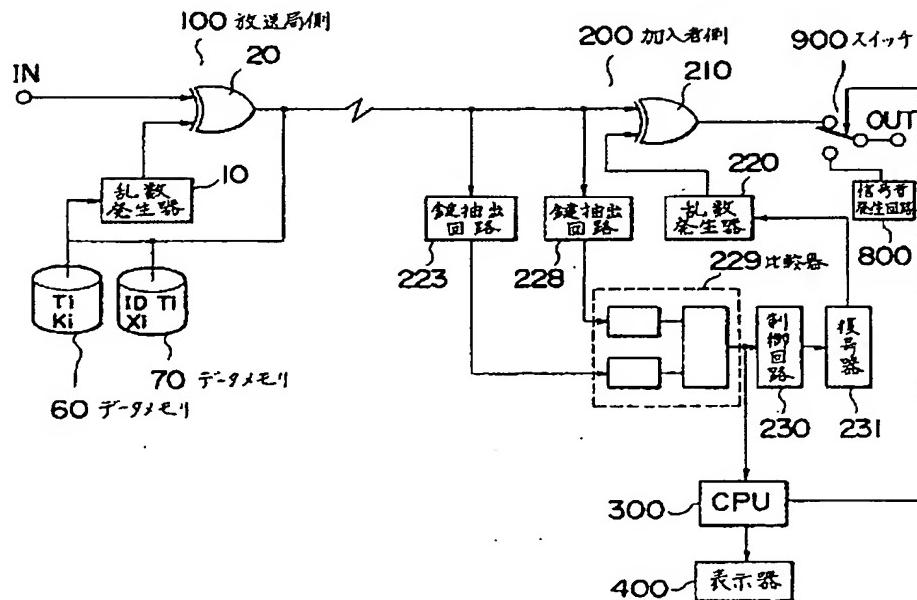
4. 図面の簡単な説明

第1図はこの発明に係る有料放送方式の実施例の概要を示す回路図、第2図及び第3図はこの発明に係る有料放送方式の実施例を示す回路図である。

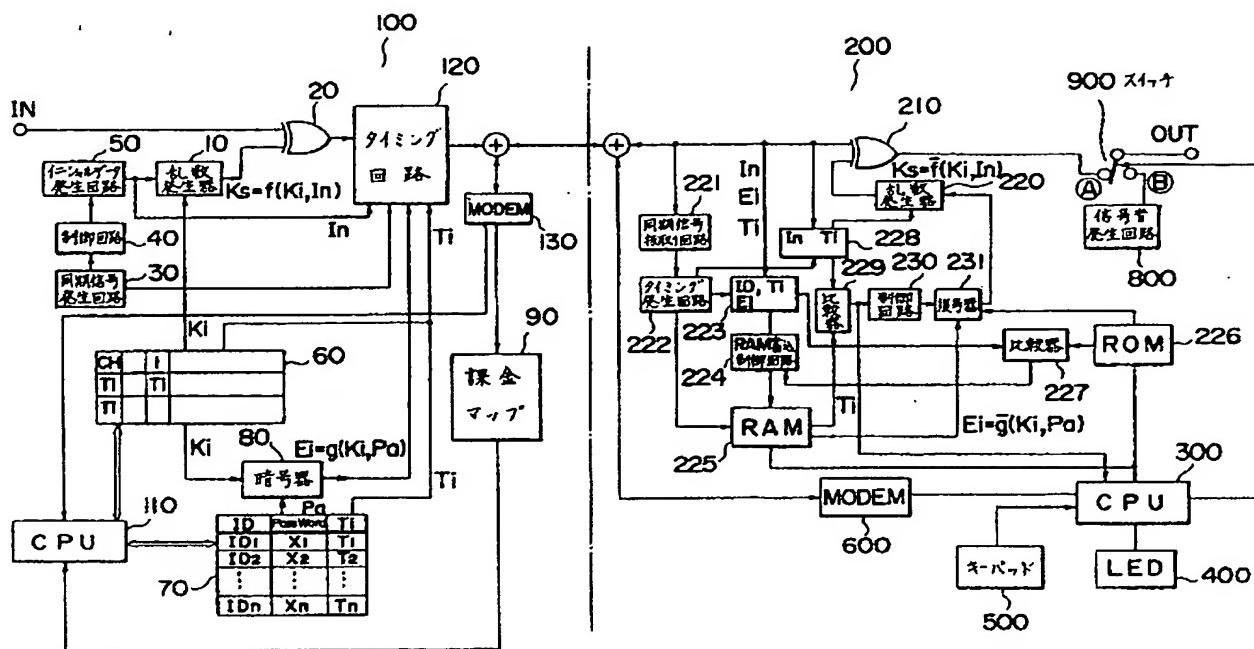
る。

- 60 … 番組種別情報発生手段、
- 70 … 契約番組種別情報発生手段、
- 80 … 鍵情報生成手段、
- 223, 228 … 抽出手段、
- 223 … 鍵情報抽出手段、
- 229 … 比較手段、
- 800 … 未契約警告手段。

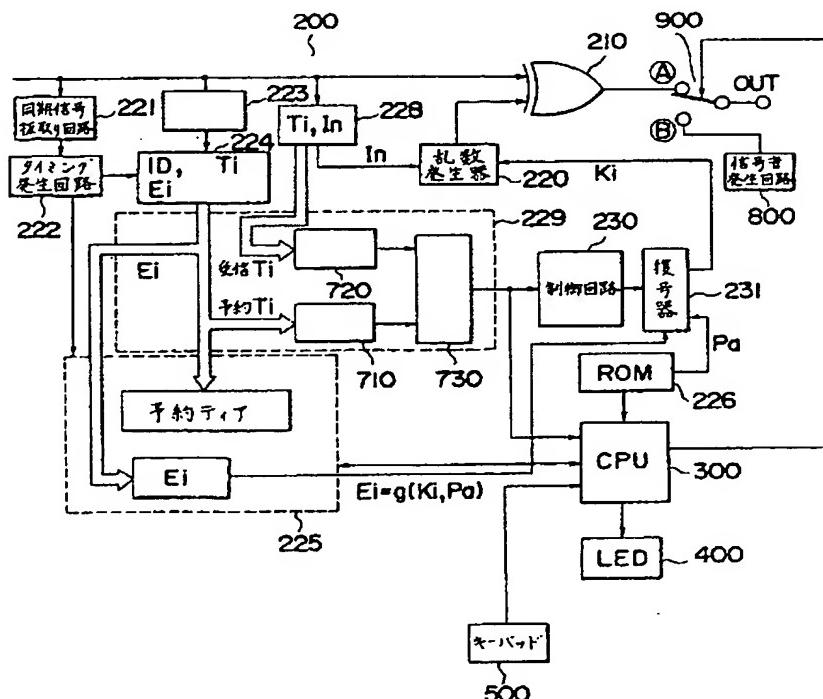
代理人弁理士 関近慧佑（ほか1名）



第1図



第2図



第3図